Christopher A. Seeger
Christopher L. Ayers
SEEGER WEISS LLP
55 Challenger Road
6th Floor
Ridgefield Park, NJ 07660

Attorneys for Plaintiff
(Additional Counsel on the Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

RAYMOND CHRISTIE, individually and on behalf of all those similarly situated, Plaintiff, v. T-MOBILE USA, INC., Defendant.	Civil Action No. **COMPLAINT and DEMAND FOR JURY TRIAL**

Plaintiff Raymond Christie ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following, against Defendant T-Mobile USA, Inc. ("T-Mobile" or "Defendant"). Based upon personal knowledge, information, belief, and investigation of counsel, Plaintiff specifically alleges as follows:

SUMMARY OF THE CASE

1. Plaintiff brings this class action on behalf of a Nationwide Class and a New Jersey Sub-Class (together, the "Classes") against Defendant because of its failure to protect the confidential personally identifying information of millions of customers—including first and last names, dates of birth, Social Security Numbers, drivers' license numbers, physical addresses, phone numbers, T-Mobile account PINs, unique International Mobile Equipment Identity (or "IMEI") numbers, and unique International Mobile Subscriber Identity (or "IMSI") numbers

(collectively, their "Personally Identifiable Information"). Defendant's wrongful disclosure has harmed Plaintiff and the Classes, which includes at least 50 million people.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) in that: (1) this is a class action involving more than 1,000 class members; (2) minimal diversity is present as Plaintiff is a citizen of New Jersey (and the proposed class members are from various states) while Defendant is a citizen of Delaware and Washington; and (3) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

3. This Court has personal jurisdiction over Defendant because it does business in and throughout New Jersey; the wrongful acts alleged in this Complaint were committed in New Jersey, among other venues; and Defendant has intentionally availed itself of this jurisdiction by marketing and selling its products and services in New Jersey.

4. Venue is proper in this District pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, and 28 U.S.C. § 1391(d) because the transactions giving rise to Plaintiff's claims occurred in Weehawken, New Jersey; and (2) 28 U.S.C. § 1391(b)(3) in that Defendant is subject to personal jurisdiction in this District.

PARTIES

5. Plaintiff Raymond Christie is an individual residing in Weehawken, New Jersey, who is (and has been since 2016) a customer of T-Mobile and whose Personally Identifiable Information, was compromised in the Data Breach described herein.

6. Defendant T-Mobile USA, Inc. ("T-Mobile") is a Delaware corporation with its principal place of business in Bellevue, Washington.

FACTUAL BACKGROUND

7. T-Mobile is a nationwide telecommunications company that provides wireless voice, messaging, and data services in the United States, Puerto Rico and the U.S. Virgin Islands under the "T-Mobile" and "Metro by T-Mobile brands." T-Mobile has over 100 million customers and annual revenues of more than $68 billion.

8. Plaintiff and other proposed Class Members were required, as current or prospective customers of T-Mobile, to provide T-Mobile with sensitive Personally Identifiable Information to apply for an/or receive T-Mobile's wireless voice, messaging, and data services.

9. On August 15, 2021, the Internet news site Vice.com first reported that T-Mobile had suffered a serious data breach. According to the article published on that date, a hacker posted to an online forum claiming to have obtained "data related to over 100 million people," which data "came from T-Mobile servers."[1] According to the article, the hacker was attempting to sell that data.

10. On the following day, August 16, 2021, T-Mobile publicly admitted that "unauthorized access to some T-Mobile data occurred." But T-Mobile stated that it had "not yet determined that there [was] any personal data involved."[2]

11. T-Mobile did not state when the unauthorized access occurred. But upon information and belief, T-Mobile learned of the breach not through its own proactive and protective cybersecurity systems, but rather as a result of the report of the hacker attempting to sell the data.

---

[1] Joseph Cox, *T-Mobile Investigating Claims of Massive Customer Data Breach*, Motherboard: Tech by Vice (Aug. 15, 2021), https://www.vice.com/en/article/akg8wg/ tmobile-investigating-customer-data-breach-100-million (last visited Aug. 25, 2021).

[2] T-Mobile Cybersecurity Incident Update (Aug. 16, 2021), https://www.t-mobile.com/news/network/cybersecurity-incident-update-august-2021 (last visited Aug. 25, 2021).

12. T-Mobile's August 16, 2021 release further stated that T-Mobile was "confident that the entry point used to gain access has been closed."[3] The fact that T-Mobile purports to have quickly located and closed the entry point suggests that, with proper precautions, T-Mobile could have eliminated the threat before the Data Breach occurred and thus prevented the theft of its customers' Personally Identifiable Information.

13. The following day, August 17, T-Mobile issued a further public statement admitting that data containing personal information had been stolen from its system. The information included that of "approximately 7.8 million current T-Mobile postpaid customer accounts . . . , as well as just over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile."[4] The announcement further stated that "approximately 850,000 active T-Mobile prepaid customer names, phone numbers and account PINs were exposed," and that "similar information from additional inactive prepaid accounts was also accessed."

14. Then, on August 20, 2021, T-Mobile issued a further release, adding that it had "identified an additional 667,000 accounts of former T-Mobile customers that were accessed with customer names, phone numbers, addresses and dates of birth compromised."[5] The release further revealed that "up to 52,000 names related to current Metro by T-Mobile accounts may have been included" among the data stolen.[6]

---

[3] *Id.*

[4] T-Mobile Shares Additional Information Regarding Ongoing Cyberattack Investigation (Aug. 17, 2021), *available at* https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation (last visited Aug. 25, 2021).

[5] T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack, (update for Aug. 20, 2021), *available at* https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation (last visited Aug. 25, 2021).

[6] *Id.*

15. On or around this time, T-Mobile sent Plaintiff and, upon information and belief, other members of the proposed class a text message stating:

> T-Mobile has determined that unauthorized access to some of your personal data has occurred. We have no evidence that your debit/credit card information was compromised. We take the protection of our customers seriously. We are taking actions to protect your T-Mobile account and we recommend that you take action to protect your credit. Read more here: t-mo.com/Protect

16. T-Mobile had obligations—created by contract, industry standards, common law, and its representations to its customers like Plaintiff and other Class Members—to keep the compromised Personally Identifiable Information confidential and to protect it from unauthorized disclosures. Plaintiff and Class Members provided their Personally Identifiable Information to T-Mobile with the understanding that T-Mobile and any business partners to whom T-Mobile disclosed the Personally Identifiable Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

17. Indeed, T-Mobile's Privacy Policy acknowledges that T-Mobile's customers "trust T-Mobile to connect [them] to the world everyday" and that they "deserve transparency . . . [and] protection," and pledges to "help [customers] take action to protect [their] privacy."[7] In the Privacy Policy, T-Mobile further promises customers to "use administrative, technical, contractual, and physical safeguards designed to protect [their] data while it is under [T-Mobile's] control."

18. Moreover, the Federal Trade Commission ("FTC") has established security guidelines and recommendations for businesses that possess their customers' sensitive personally

[7] T-Mobile Privacy Notice (effective May 5, 2021), https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last visited Aug. 25, 2021).

identifiable information to reduce the likelihood of data breaches.[8] Among such recommendations are: limiting the sensitive consumer information kept; encrypting sensitive information sent to third parties or stored on computer networks; and identifying and understanding network vulnerabilities.

19. Defendant's data security obligations and promises were particularly important given the substantial increase in data breaches preceding August 2021, which were widely known to the public and to anyone in the telecommunications industry.

20. Moreover, T-Mobile itself has been particularly aware of the vulnerability of its security systems, having previously suffered four data breaches over the past three years. Specifically, in August 2018, information for two million T-Mobile customers was compromised.[9] In November 2019, information for one million T-Mobile prepaid customers was compromised.[10] In March 2020, an unknown number of T-Mobile's customers' names, addresses, phone numbers, account numbers, rate plans and features, and billing information was compromised.[11] And in early December 2020, T-Mobile discovered that the Personally Identifiable Information of about 200,000 customers was compromised.[12]

---

[8] *See* Federal Trade Commission, *Protecting Personal Information*: *A Guide for Business* (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 25, 2021

[9] *See* Alicia Hope, *Second Data Breach in 2020 for T-Mobile Exposed Customer and Call-Related Information of 200,000 Subscribers*, CPO Magazine (Jan. 11, 2021), *available at* https://www.cpomagazine.com/cyber-security/second-data-breach-in-2020-for-t-mobile-exposed-customer-and-call-related-information-of-200000-subscribers/ (last visited Aug. 26, 2021).

[10] *Id.*

[11] *See T-Mobile's Data Breach Exposes Customer's Data and Financial Information*, Security (Mar. 6, 2020), https://www.securitymagazine.com/articles/91856-t-mobiles-data-breach-exposes-customers-data-and-financial-information (last visited Aug. 26, 2021).

[12] *See* Alicia Hope, *Second Data Breach in 2020 for T-Mobile Exposed Customer and Call-Related Information of 200,000 Subscribers*, CPO Magazine (Jan. 11, 2021), *available at* https://www.cpomagazine.com/cyber-security/second-data-breach-in-2020-for-t-mobile-exposed-customer-and-call-related-information-of-200000-subscribers/ (last visited Aug. 26, 2021).

21. Additionally, in 2017, a security researcher found a glitch on a T-Mobile website that allowed hackers to access the Personally Identifiable Information of a customer, including his or her email addresses, account numbers, and IMSI numbers, if they knew the customer's phone number.[13] The researcher stated that "T-Mobile has 76 million customers, and an attacker could have ran a script to scrape the data (email, name, billing account number, IMSI number, other numbers under the same account which are usually family members) from all 76 million of these customers to create a searchable database with accurate and up-to-date information of all users."[14] T-Mobile had no mechanism in place to prevent this type of data breach.

22. Consumers have choices for wireless voice, messaging, and data services and they would not have chosen to provide their Personally Identifiable Information to T-Mobile had they known that the information would be at heightened risk of compromise due to T-Mobile's lax data security.

23. Defendant's repeated security failures demonstrate that it failed to honor their duties and promises by not, among other things:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting Plaintiff's and the Classes' Personally Identifiable Information;

c. Failing to reasonably limit the sensitive consumer information kept, in violation of FTC recommendations; and

[13] Lorenzo Franceschi-Bicchierai, *T-Mobile Website Allowed Hackers to Access Your Account Data With Just Your Phone Number*, Motherboard: Tech by Vice (Oct. 10, 2017), https://www.vice.com/en/article/wjx3e4/t-mobile-website-allowed-hackers-to-access-your-account-data-with-just-your-phone-number (last accessed Aug. 26, 2021).

[14] *Id.*

d. Failing to encrypt sensitive information sent to third parties or stored on computer networks, in violation of FTC recommendations.

It is Well-Established That Data Breaches Lead to Identity Theft

24. Plaintiff and other Class Members have been injured by the disclosure of their Personally Identifiable Information in the Data Breach.

25. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[15] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

26. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[16]

27. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as social security numbers ("SSNs") for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/finance fraud.

28. There may be a time lag between when Personally Identifiable Information is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft.* Further, once stolen data have been sold or posted on

[15] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* https://www.gao.gov/new.items/d07737.pdf (last visited Aug. 25, 2021).

[16] *Id*. at 2, 9

> the Web, *fraudulent use of that information may continue for years.* As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

29. With access to an individual's Personally Identifiable Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[18]

30. Personally Identifiable Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Personally Identifiable Information directly on various Internet websites making the information publicly available.

CLASS ALLEGATIONS

31. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff brings this case as a class action on behalf of a Nationwide Class and a New Jersey Sub-Class, defined as follows**:**

> Nationwide Class: All persons in the United States whose Personally Identifiable Information was maintained on the T-Mobile systems that

[17] *Id*. at 29 (emphasis supplied).

[18] *See Federal Trade Commission,* Warning Signs of Identify Theft, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Aug. 25, 2019).

were compromised as a result of the breach announced by T-Mobile on or around August 16, 2021.

New Jersey Sub-Class: All persons in the State of New Jersey whose Personally Identifiable Information was maintained on the T-Mobile systems that were compromised as a result of the breach announced by T-Mobile on or around August 16, 2021.

32. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

33. There are numerous questions of law and fact common to Plaintiff and Class Members. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant owed Plaintiff and other Class Members a duty to implement and maintain reasonable security procedures and practices to protect their Personally Identifiable Information, and whether it breached that duty;

b. Whether Defendant continues to breach duties to Plaintiff and the other Class Members

c. Whether Defendant's data security systems prior to the Data Breach met industry standards;

d. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay;

e. Whether Plaintiff's and other Class members' Personally Identifiable Information was compromised in the Data Breach; and

f. Whether Plaintiff and other Class Members are entitled to damages as a result of Defendant's conduct.

34. Plaintiff's claims are typical of the claims of the Classes' claims. Plaintiff suffered the same injury as Class Members—*i.e.*, Plaintiff's Personally Identifiable Information was compromised in the Data Breach.

35. Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiff nor his counsel has interests that are contrary to or that conflict with those of the proposed Classes.

36. Defendant has engaged in a common course of conduct toward Plaintiff and other Class Members. The common issues arising from this conduct that affect Plaintiff and Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

37. A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the prosecution of separate actions is low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendant. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties.

Defendant's records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiff's claims.

38. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant has acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

FIRST COUNT
Negligence
(On behalf of Plaintiff, the Nationwide Class, and the New Jersey Sub-Class)

39. Plaintiff realleges and incorporates by reference all preceding factual allegations.

40. T-Mobile required Plaintiff and Class Members to submit non-public Personally Identifiable Information to obtain its telecommunications services.

41. By collecting and storing this data, and sharing it and using it for commercial gain, Defendant both had a duty of care to use reasonable means to secure and safeguard this Personally Identifiable Information, to prevent disclosure of the information, and to guard the information from theft.

42. Defendant's duty included a responsibility to implement a process by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

43. Defendant also owed a duty of care to Plaintiff and members of the Classes to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that their systems and networks—and the personnel responsible for them adequately protected their customers' Personally Identifiable Information.

44. Defendant's duty to use reasonable security measures arose as result of the special relationship that existed between it and its customers. Only Defendant was in a position to

ensure that its systems were sufficient to protect against the harm to Plaintiff and the members of the Classes from a data breach.

45. In addition, Defendant had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

46. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the common law, statutes, and FTC guidance described above, but also because they are bound by, and have committed to comply with, industry standards for the protection of confidential Personally Identifiable Information.

47. Defendant breached its common law, statutory and other duties—and thus, were negligent—by failing to use reasonable measures to protect its customers' Personally Identifiable Information, and by failing to provide timely notice of the Data Breach.

48. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Personally Identifiable Information;

b. allowing unauthorized access to Plaintiff's and Class Members' Personally Identifiable Information;

c. failing to recognize in a timely manner that Plaintiff's and other Class Members' Personally Identifiable Information had been compromised; and

d. failing to warn Plaintiff and other Class Members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

49. It was foreseeable that Defendant's failure to use reasonable measures to protect Personally Identifiable Information and to provide timely notice of the Data Breach would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Classes were reasonably foreseeable.

50. It was therefore foreseeable that the failure to adequately safeguard Personally Identifiable Information would result in one or more of the following injuries to Plaintiff and the members of the proposed Classes: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

51. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an order declaring that Defendant's conduct constitutes negligence and awarding damages in an amount to be determined at trial.

SECOND COUNT
Breach of Implied Contract
(On behalf of Plaintiff, the Nationwide Class, and the New Jersey Sub-Class)

52. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

53. When Plaintiff and Class Members paid money and provided their Personally Identifiable Information to Defendant in exchange for services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

54. Defendant solicited and invited prospective customers to provide their Personally Identifiable Information as part of its regular business practices. These individuals accepted Defendant's offers and provided their Personally Identifiable Information to Defendant. In entering into such implied contracts, Plaintiff and the Class Members assumed that Defendant's data security practices and policies were reasonable and consistent with industry standards, and that Defendant would use part of the funds received from Plaintiff and the Class Members to pay for adequate and reasonable data security practices.

55. Plaintiff and the Class Members would not have provided and entrusted their Personally Identifiable Information to Defendant in the absence of the implied contract between them and Defendant to keep the information secure.

56. Plaintiff and the Class Members fully performed their obligations under the implied contracts with Defendant.

57. Defendant breached its implied contracts with Plaintiff and the Class Members by failing to safeguard and protect their Personally Identifiable Information and by failing to provide

timely and accurate notice that their personal information was compromised as a result of a data breach.

58. As a direct and proximate result of Defendant's breaches of its implied contracts, Plaintiff and the Class Members sustained actual losses and damages as described herein.

THIRD COUNT
Misrepresentation
(On behalf of Plaintiff, the Nationwide Class, and the New Jersey Sub-Class)

59. Plaintiff realleges and incorporates by reference each of the allegations set forth above.

60. Defendant falsely represented to Plaintiff and Class Members that it would take appropriate and reasonable measures to safeguard their Personally Identifiable Information and promptly notify them of a data breach.

61. Plaintiff and Class members reasonably relied upon said representations in that they provided Defendant their Personally Identifiable Information.

62. Defendant's misrepresentations were material, as Plaintiff and Class Members would not have chosen to provide their Personally Identifiable Information to T-Mobile had they known that the information would be at heightened risk of compromise due to T-Mobile's lax data security.

63. As a result of Defendant's misrepresentations, Plaintiff and the Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personally Identifiable Information, and thereby suffered ascertainable economic loss.

FOURTH COUNT
Violation of the New Jersey Consumer Fraud Act
N.J. Stat. Ann. § 56:8-1, et seq.
(On behalf of Plaintiff and the New Jersey Sub-Class)

64. Plaintiff realleges and incorporates by reference each of the allegations set forth above.

65. Plaintiff and all Class members are "consumers" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1.

66. The Defendant is a "person" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1(d).

67. Defendant's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by N.J.S.A. 56:8-1.

68. Defendant advertised, offered, or sold goods or services in New Jersey and engaged in trade or commerce directly or indirectly affecting the citizens of the State of New Jersey.

69. Defendant solicited Plaintiff and Class Members to do business and uniformly and knowingly misrepresented to that by joining, their Personally Identifiable Information was safe, confidential and protected from intrusion, hacking or theft.

70. Defendant misrepresented that it would protect the privacy and confidentiality of Plaintiff' and Class Members' Personally Identifiable Information, including by implementing and maintaining reasonable security measures.

71. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on their misrepresentations and omissions.

72. Defendant failed to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' Personally Identifiable Information in violation of N.J.S.A. 56:8-162, which was a direct and proximate cause of the Data Breach.

73. Defendant failed to provide notice to Plaintiff and Class Members or otherwise comply with the notice requirements of N.J.S.A. 56:8-163.

74. Defendant's acts and omissions, as set forth herein, evidence a lack of good faith, honesty in fact and observance of fair dealing, so as to constitute unconscionable commercial practices, in violation of N.J.S.A. 56:8-2.

75. As a direct and proximate result of Defendant' unfair and deceptive acts and practices, Plaintiff and Class Members are required to expend sums to protect and recover their Personally Identifiable Information, have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personally Identifiable Information, and thereby suffered ascertainable economic loss.

76. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

FIFTH COUNT
Violation of the New Jersey Consumer Security Breach Disclosure Act
N.J. Stat. Ann. § 56:8-163, et seq.
(On behalf of Plaintiff and the New Jersey Sub-Class)

77. Plaintiff realleges and incorporates by reference each of the allegations set forth above.

78. Under N.J. Stat. Ann. § 56:8-163(a), "[a]ny business that conducts business in New Jersey . . . that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was,

or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay[.]"

79. T-Mobile is a business that conducts business in New Jersey that compiles or maintains computerized records that include personal information under N.J. Stat. Ann. § 56:8-163(a).

80. The Personally Identifiable Information of Plaintiff and the members of the New Jersey Sub-Class that was compromised in the T-Mobile Breach includes personal information covered under N.J. Stat. Ann. §§ 56:8-163, *et seq*.

81. Because T-Mobile discovered a breach of its security system in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured, T-Mobile had an obligation to disclose the T-Mobile Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, *et seq*.

82. By failing to disclose the T-Mobile Breach in a timely and accurate manner, T-Mobile violated N.J. Stat. Ann. § 56:8-163(a).

83. As a direct and proximate result of T-Mobile's violations of N.J. Stat. Ann. § 56:8-163(a), Plaintiff and the New Jersey Sub-Class members suffered the damages described above.

84. Plaintiff and the New Jersey Sub-Class members seek relief under N.J. Stat. Ann. § 56:8-19, including but not limited to treble damages (to be proven at trial), attorneys' fees and costs, and injunctive relief.

WHEREFORE, Plaintiff and Class Members demand judgment as follows:

A. Certification of the action as a Class Action pursuant to Federal Rule of Civil Procedure 23, and appointment of Plaintiff as Class Representative and his counsel of record as Class Counsel;

B. That acts alleged herein be adjudged and decreed to constitute negligence and violations of the consumer protection laws of New Jersey;

C. A judgment against Defendant for the damages sustained by Plaintiff and the Classes defined herein, and for any additional damages, penalties, and other monetary relief provided by applicable law;

D. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes, including, but not limited to:

a Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d Ordering that Defendant segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, unauthorized third parties cannot gain access to other portions of Defendant's systems;

e Ordering that Defendant purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

f Ordering that Defendant conduct regular database scanning and securing checks; and

g Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

E. By awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of the Complaint in this action;

F. The costs of this suit, including reasonable attorney fees; and

G. Such other and further relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of all those similarly situated, hereby requests a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

Dated: August 27, 2021

Respectfully submitted,

/s/ Christopher A. Seeger

Christopher A. Seeger
Christopher L. Ayers
SEEGER WEISS LLP
55 Challenger Road
6th Floor
Ridgefield Park, NJ 07660
cseeger@seegerweiss.com
cayers@seegerweiss.com

James E. Cecchi
Kevin G. Cooper
CARELLA, BYRNE, CECCHI, OLSTEIN, BRODY & AGNELLO, P.C.

5 Becker Farm Road
Roseland, New Jersey 0768
Telephone: (973) 994-1700
Facsimile: (973) 994-1744
jcecchi@carellabyrne.com
kcooper@carellabyrne.com

Joseph H. Meltzer
Melissa L. Troutner
KESSLER TOPAZ MELTZER & CHECK, LLP
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7756
jmeltzer@ktmc.com
mtroutner@ktmc.com

Counsel for Plaintiff and the Proposed Classes